EXHIBIT Z

IN THE UNITED STATES DISTRICT COURT
EASTERN DISTRICT OF VIRGINIA
ALEXANDRIA DIVISION

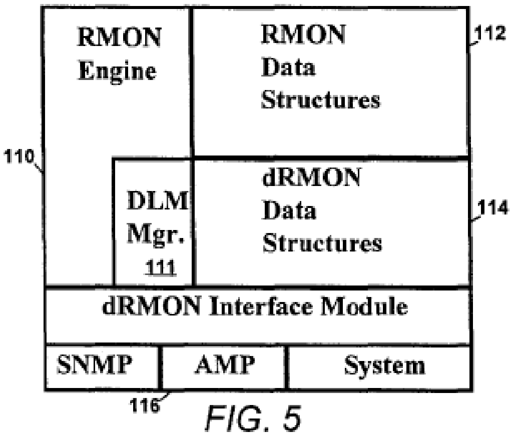
AMDOCS (ISRAEL) LIMITED, an Israeli Corporation, Plaintiff, v. OPENET TELECOM, INC., a Delaware Corporation, and OPENET TELECOM LTD., an Irish Corporation, Defendants.	Case No. 1:10cv910 (LMB/TRJ)

EXPERT REPORT OF PATRICK MCDANIEL REGARDING INVALIDITY

Appendix B – Invalidity Analysis Claim Charts for '510 Patent

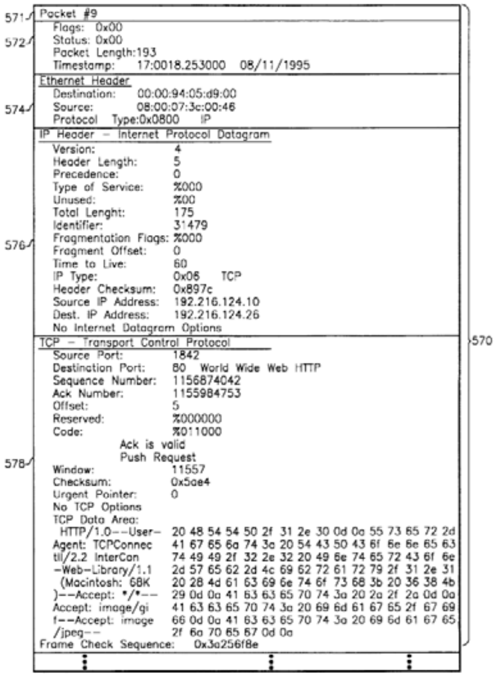
Concord and the '169 Patent

U.S. Patent No. 7,412,510	Concord Communication's Network Health
16. A computer program product stored in a computer readable medium for reporting on a collection of network usage information from a plurality of network devices, comprising:	The Concord Datasheet describes a software application, referred to as Network Health, which collects network usage data. "The Network Health family of turnkey reporting applications automates the collection, analysis, and reporting of critical network data.", [1], Page 1. "A software-only solution, Network Health does not require any additional probes or agents.", [1], Page 2. "Software-only solution", [1], Page 3. "Software-only, automated solution is easily deployed in large networks", [3], Page 1. See also the required hardware specification [1], Page 2. "Network Health runs on both the Sun SPARC and HP 9000 platforms.", [1], Page 4.
computer code for collecting network communications usage information in real-time from a plurality of network devices at a plurality of layers;	The Concord Datasheet describes a method used by Network Health of collecting network usage data. "The Network Health family of turnkey reporting applications automates the collection, analysis, and reporting of critical network data.", [1], Page 1. "..., Network Health discovers and collects vital data from ...", [1], Page 1. "SNMP-based polling enables the collection of information from existing devices in the network, leveraging your equipment investment.", [1], Page 2. "... and automatically collects, analyzes and distills the information down to key points.", [1], Page 4. "Support for standards such as SNMP, MIBII, and RMON, coupled with an extensive library of supported devices saves your support team time and resources.", [1], Page 4. "SNMP enables the collection of information from existing devices in the network, ...", [2], Page 1. Furthermore, this network data can come from a multitude of network devices and encompass network usage information. "... data from devices already installed on your network - bridges, routers, switches, RMON agents, local segments and wide area links ...", [1], Page 1.

	packets flowing on the network are captured for later analysis." Column 8, Lines 59 – 61. The 243 Patent describes how information can be aggregated to create statistics by the dRMON agents. "According to the invention, on a regular, periodic basis the dRMON agents forward their statistics and/or captured packets to a dRMON proxy or collector, existing somewhere on the WAN/LAN." Column 6, Lines 10 – 13. Finally, the dRMON is also capable of aggregating the collected information. "The dRMON Proxy receives RMON analysis and capture data from the agents and sorts, collates, and aggregates that information into a cohesive database that recreates the view a prior art RMON probe would have if the ESs were all on the same LAN segment with the prior art probe." Column 8, Lines 45 – 49.
computer code for completing a plurality of data records from the filtered and aggregated network communications usage information, the plurality of data records corresponding to network usage by a plurality of users;	The 243 Patent describes how data records can be completed by correlating the collected information. "The proxy combines received agent data thereby creating ..." Column 6, Lines 13 – 14. Furthermore, the 243 Patent describes the merging of collected information. "The Integrator 148 merges RMON statistics, tables and capture streams coming from the remote dRMON agents with the equivalent output from the Proxy's analysis of its own directed traffic combined with the broadcast and multicast traffic present at its interface." Column 9, Lines 38 – 42. "A DP merges and organizes this various information to create a seemingly homogenous view of its management domain." Column 12, Lines 66 – 1.
computer code for storing the plurality of data records in a database;	The 243 Patent describes how a database is used to store collected information. "Data structures and tables are built and maintained within the section labeled RMON Data Structures 112." Column 8, Lines 16 – 18.  RMON Engine RMON Data Structures 112 110 DLM Mgr. 111 dRMON Data Structures 114 dRMON Interface Module SNMP AMP System 116 FIG. 5

	described, it is understood that the packet capturing module 322 may be arranged to filter by other criteria such as by the protocol which describes a service such as FTP or HTTP and that the criteria for filtering may be found in the any available field in the raw packet data profile 500." Column 8, Lines 55 – 61. "The filters 344 may be applied to the data to remove packets which do not include port 80 as either a source or destination." Column 10, Lines 37 – 39. The 253 Patent describes how aggregation, in the form of addition or summation, can be performed on the communications usage information. "The number of bits traversing the network medium may be calculated from data provided through the network interface 316 and this number is counted over a given time period." Column 12, Lines 15 – 18.
computer code for completing a plurality of data records from the filtered and aggregated network communications usage information, the plurality of data records corresponding to network usage by a plurality of users;	The 253 Patent describes how data records can be completed by correlating, referred to as grouping and segregating, the filtered and aggregated network communications usage information. "First, the data may be sorted by nodes in a transaction and then each transaction may be recompiled into the proper sequence. Preferably, hashing techniques may be used to group the data, but the artisan will recognize alternative techniques." Column 10, Lines 46 – 50. "Additionally, the entries are segregated according to the packets exchanged between the selected ports." Column 10, Lines 53 – 55. Furthermore, the 253 Patent describes an example of how data records can be completed by correlating and subsequently merging the filtered and aggregated network communications usage information. "Additionally, by communicating with the Internet through, for example, the remote access interface 310, information about nodes can be determined. Specifically, suppose a node is generating activity for which inquiry is desired. By transmitting a reverse DNS (Domain Name Service) Query, the IP address field (typically a string of numbers) can be used to provide its Internet address. Thus, an e-mail or other warning could be sent to that user. Additionally, by accessing the IP addresses of the users that visit a site and using the reverse DNS lookup, visitors can be classified in terms of country, commercial, educational, or government. Moreover, using readily available Internet resources, a variety of information beyond the domain name may be ascertained." Column 12, Lines 46 – 59. Finally, the 253 Patent describes an example of how data records can be completed, or derived, using network communications usage information. "Referring now to FIG. 5c, an entry 570 for a sample data table 569 derived from data provided in the decoded packet data buffer 338 is shown to include ..." Column 9, Lines 50 – 52.

<table>
<tr>
<td></td>
<td>



```
Packet #9
   Flags:  0x00
   Status: 0x00
   Packet Length:193
   Timestamp:     17:0018.253000   08/11/1995
Ethernet Header
   Destination:     00:00:94:05:d9:00
   Source:          08:00:07:3c:00:46
   Protocol   Type:0x0800     IP
IP Header - Internet Protocol Datagram
   Version:              4
   Header Length:        5
   Precedence:           0
   Type of Service:      %000
   Unused:               %00
   Total Lenght:         175
   Identifier:           31479
   Fragmentation Flags:  %000
   Fragment Offset:      0
   Time to Live:         60
   IP Type:              0x06    TCP
   Header Checksum:      0x897c
   Source IP Address:    192.216.124.10
   Dest. IP Address:     192.216.124.26
   No Internet Datagram Options
TCP - Transport Control Protocol
   Source Port:          1842
   Destination Port:     80  World Wide Web HTTP
   Sequence Number:      1156874042
   Ack Number:           1155984753
   Offset:               5
   Reserved:             %000000
   Code:                 %011000
            Ack is valid
            Push Request
   Window:               11557
   Checksum:             0x5ae4
   Urgent Pointer:       0
   No TCP Options
   TCP Data Area:
    HTTP/1.0--User-   20 48 54 54 50 2f 31 2e 30 0d 0a 55 73 65 72 2d
   Agent: TCPConnec   41 67 65 6a 74 3a 20 54 43 50 43 6f 6e 6e 65 63
   til/2.2 InterCon   74 49 49 2f 32 2e 32 20 49 6e 74 65 72 43 6f 6e
   -Web-Library/1.1   2d 57 65 62 2d 4c 69 62 72 61 72 79 2f 31 2e 31
    (Macintosh: 68K   20 28 4d 61 63 69 6e 74 6f 73 68 3b 20 36 38 4b
   )--Accept: */*--   29 0d 0a 41 63 63 65 70 74 3a 20 2a 2f 2a 0d 0a
   Accept: image/gi   41 63 63 65 70 74 3a 20 69 6d 61 67 65 2f 67 69
   f--Accept: image   66 0d 0a 41 63 63 65 70 74 3a 20 69 6d 61 67 65
   /jpeg--            2f 6a 70 65 67 0d 0a
Frame Check Sequence:    0x3a256f8e
```

FIG. 5c

</td>
</tr>
<tr>
<td>computer code for storing the plurality of data records in a database;</td>
<td>

The 253 Patent describes many concepts for storing data that are typically associated with databases, such as “tables”, “fields”, and “indexing”.

“The data management and storage section 210 also conserves data storage space by filtering the decoded data to limit it to a desired set and indexing the data to avoid redundant storage of the same data. The data management and storage section 210 also manages the long term storage of the data.” Column 5, Lines 31 – 36.

“Referring now to FIG. 5b, a sample data table 550 derived from data provided in the raw packet data buffer 334 is shown to include packet identity 555, source physical 557, destination physical 559, size 559 and time stamp 561 fields for a plurality of sample entries. Specifically, the table in FIG. 5b shows a list of packets received promiscuously between two locations.” Column 9, Lines 6 – 12.

</td>
</tr>
</table>

	being passed from or to these servers will be detected and stored by the agent." Col 3, Line 18 "As the agents are aware of the application protocols, the systems are capable of collecting useful data for trouble-shooting, trend analysis, resource planning, security auditing, accounting and chargeback, and other applications." Col 3, Line 27 "Each of the agents can continuously monitor in real time business transactions, databases, systems and networks detecting and correlating events, initiating corrective actions, and providing event notifications." Col 6 Line 22
computer code for filtering and aggregating the network communications usage information;	The 010 patent discloses filtering and aggregating the network communications usage information. "and a filter module for processing the data to detect portions of that data which is representative of communications associated with that server program. The system can further include a data memory for storing the detected portions of data." Col 3, Line 40 "The system can further comprise a control module for providing a list of a plurality of server programs and for generating a plurality of the filter modules, each one of which can be associated with a respective one of the plurality of server programs." Col 3, Line 65 "In this way, the module 80 can filter from the traffic those portions that are relevant to the agent 50 and pass copies of this traffic to the agent 50." Col 8, Line 15 "The system can also include an agent for coupling into the data memory and for processing the detected portions of data to generate information representative of an operation of the server program." Col 3, Line 45
computer code for completing a plurality of data records from the filtered and aggregated network communications usage information, the plurality of data records corresponding to network usage by a plurality of users;	The 010 patent discloses completing a plurality of data records. "Each of the agents can continuously monitor in real time business transactions, databases, systems and networks detecting and correlating events, initiating corrective actions, and providing event notifications." Col 6, Line 23 "The agent 50 includes an external event interface 52, a communications interface 54, a tools interface 58, and MUM console interface 60, and event correlation processor 64, a system monitor 70, a network monitor 72, a SYBASE.TM. client monitor 74, and a SYBASE.TM. server monitor 76. The overall architecture of the agent 50 shows that the agent includes a set of monitor elements 70-76 and an external events interface 52 that provide event information about various components of the enterprise to the correlation processor 64. The correlation processor 64 correlates the events to generate data that can be passed to the MUM console 42, or passed to other tools, including other management tools or instrumentation code for setting off alarms, activating a beeper, sending a fax via modem, sending e-mail to system administrators or taking corrective action. Accordingly, the agent 50 collects details of events and processes these details in the correlation processor 64 to generate information representative, among other things, of business transactions." Col 6, Line 46